UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/573,220	02/27/2007	Qibin Sun	121187-827-NP	5054

24964 7590 12/15/2008

GOODWIN PROCTER LLP
ATTN: PATENT ADMINISTRATOR
620 Eighth Avenue
NEW YORK, NY 10018

EXAMINER	
BITAR, NANCY	

ART UNIT	PAPER NUMBER
2624	

MAIL DATE	DELIVERY MODE
12/15/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/573,220	SUN ET AL.	
	Examiner	Art Unit	
	NANCY BITAR	2624	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 March 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *25-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *25-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 March 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/20/06,2/1/07,9/29/08*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Examiner Notes

1. Examiner cites particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, the applicant fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Claim Objections

2. Claims 42-44 are objected to because of the following informalities: The claim recites "any one of claim 36" and claim 36 is a single claim. Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) The invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 25-50 are rejected under 35 U.S.C. 102 (b) as being anticipated by CHANG ET al (WO 03/030541).

As to claim 25, CHANG et al teaches a method of protecting a digital image, the method comprising:

extracting feature values from the digital image based on a selected authentication bit-rate and a selected image content (one or more feature codes are derived from a first set of data that is to be watermarked. One or more parity checks bits are derived from the feature codes and are included in one or more codeword, page 5; lines 15-31);

selecting an authentication mode for processing the extracted feature values,

the processing of the extracted (authentication system, watermark data 828 are extracted by block 826 from the watermarked content 824 using the same secret key 816 as was used in the watermarking system illustrated in Fig. 8A. If a randomization step 808 was used in the original watermarking procedure, the watermark data 828 is decoded/unrandomized by block 830 in the authentication system to derive unrandomized data 832; figure 8b; page 4; note that there is no characterization in the claims of how the processing of extracted feature values is affected by which mode is selected) feature values comprising deriving data corresponding to the extracted feature values based on the selected authentication mode (watermark data 828);

and creating an image signature based on the data corresponding to the feature values (image domain data 102; The block diagram illustrates the processing of image data, but the watermarking and authentication methods of the present invention can be applied to a variety of different types of data including, but not limited to, image data, video data, audio data, and/or other multimedia data, figure 1).

As to claim 26, CHANG et al teaches the method as claimed in claim 25, wherein the processing comprises correcting coding (ECC) the extracted feature values to derive the data corresponding to the feature values (user selectable authentication bit rate constitutes the step of selecting a desired authentication robustness level" as per claim 2 since the authentication bit rate affects the robustness of the embedded watermark; see abstract).

As to claim 27, CHANG et al teaches the method as claimed in claim 25, wherein the feature values from each of a plurality of code blocks of the original digital image are thresholded and coded to create the data corresponding to the feature values (The newly derived feature codes 306 are therefore compared on a subblock-by-subblock basis to the corresponding message codes 350 derived from the extracted watermarks 310 (step 312). For each feature code and message code being compared, the comparison procedure 312 determines whether the PCBs associated with the message code equal the PCBs associated with the feature code).

As to claim 28, CHANG et al teaches the method as claimed in any one of claim 25, wherein the processing further comprises embedding the data corresponding to the feature values into the digital image (note that the processing section 910 and/or its components can be incorporated into an imager such as a digital video camera or a digital still-image camera; pages 21-23).

As to claim 29, CHANG et al teaches the method as claimed in claim 26, further comprising applying ECC coding again to parity check bits generated during the ECC

coding of the extracted feature values to generate the data corresponding to the feature values (figure 3).

As to claim 30, CHANG et al teaches the method as claimed in claim 28, wherein the embedding of the data corresponding to the feature values as a watermark is conducted in a lossy or a lossless way, based on the selected authentication mode (Turning back to Fig. 2A, typically not all of the available bit planes are used for deriving the feature codes 204. Rather, the percentage of bits to be used for deriving feature codes is equal to an authentication bit rate 242 which can be selected by the user, pages 17-18).

As to claim 31, CHANG et al teaches the method as claimed in any one of claim 25, wherein the creating of the image signature comprises applying a cryptographic hashing function to a bit sequence representing the data corresponding to the feature values (note that feature code can be a data set representing an edge map of an image, a data set representing a brightness histogram of an image, or a sequence of bits from a rectangular region of a single bit plane of encoded, transform-domain image data; Fig. 14. In image and/or audio compression applications, such functions are commonly used to represent the amount of distortion D as a function of" bit rate; see also figure 12A; 12B).

As to claim 32, CHANG et al teaches the method as claimed in any one of claim 25, wherein the creating of the image signature comprises utilizing a private key (private key 708, figure 7A).

As to claim 33, CHANG et al teaches the method as claimed in any one of claim 25, wherein the method further comprises distributing the digital image, including the embedded data, as the authentic digital image (note that the secret key 816 must be distributed to any party who will be authenticating data, and this requirement increases the risk that the secrecy of the key 816 will be compromised, pages 5 and6)

As to claim 34, CHANG et al teaches the method as claimed in any one of claim 25, further comprising coding the digital image, including the embedded data, utilizing JPEG2000 compression (EBCOT is, in fact, the compression engine used in the well known JPEG2000 image encoding standard, which is described in Information Technology--JPEG2000 Image Coding System, ISO/IEC International Standard 15444-1 (Dec. 2000). In the system and procedure illustrated in Fig. 1, the EBCOT encoding by block 112 produces a set of EBCOT codes 118; figure 5).

As to claim 35, CHANG et al teaches the method as claimed in claim 34, wherein the extracting of the feature values, the embedding of the data corresponding to the feature values, and the creating of the image signature are performed as part of the JPEG 2000 coding (JPEG2000 image encoding standard; page 9 lines 10-27).

As to claim 36, CHANG et al teaches the method of authenticating a digital image, the method comprising: extracting feature values from the digital image based on a selected authentication bit-rate; and processing the extracted feature values to derive

data corresponding to original feature values based on a selected

authentication mode; and comparing the derived data corresponding to the

original feature values with reference data derived from an image signature associated with the digital image (comparison procedure 312; note that the decrypted signature 336 is then compared to the newly derived digest 324 on a bit-by- bit basis by block 326 to derive an authentication result 328. The authentication result 328 indicates whether the watermarked EBCOT codes 302 have been fraudulently manipulated; see page 21, lines 5-28).

As to claim 37, CHANG et al teaches the method as claimed in claim 36, wherein deriving the data corresponding to the feature values comprises ECC coding the extracted data and extracted feature values (a set of ECC codewords 358 is extracted by block 330 from the wavelet transform coefficients 356 that were derived from the EBCOT codes 302 by block 354; figure 3; pages 21-23).

As to claim 38, CHANG et al teaches the method as claimed in claim 36, wherein the extracted feature values from each of a plurality of code blocks of the digital image are decoded to derive the data corresponding to the original feature values (The extracted ECC codewords 358 are decoded using an error correction decoding (i. e. , inverse ECC) procedure 360 to derive a decoded second stage watermark 33; figure 3; pages 21-23)..

As to claim 39, CHANG et al teaches the method as claimed in any one of claim 36, further comprising extracting data embedded as a watermark in the digital image; and the processing the extracted data and the extracted feature values to derive the data corresponding to original feature values (The watermarked data 638 are then inverse transformed (block 614) to derive a watermarked version 616 of the original

content 604. For example, if the original content 604 is a set of image-domain data, the watermarked content 616 is typically also a set of image-domain data; see figure 5).

As to claim 40, CHANG et al teaches the method as claimed in claim 37, further comprising applying ECC decoding twice to the extracted data (each group PCB within the resulting set of PCBs 340 is then decoded by an error correction decoding procedure 348 to generate a message code; page 22; lines 8 to page 23 lines 1-30).

The limitation of claims 41-45 has been addressed above.

As to claim 46, CHANG et al teaches the method as claimed in claim 36, wherein the extracting of the data embedded as a watermark, the extracting of feature values from the digital image, the processing of the extracted data and extracted feature values, and the comparing of the derived data corresponding to the original feature values with the reference data are performed as part of the JPEG 2000 de-coding (The decoded second stage watermark 332-which is a signature extracted from the wavelet transform coefficients 356 derived from the watermarked EBCOT codes 302-is decrypted by block 334 using a PKI public key 344 which corresponds to the private key 232 used to encrypt the digest by block 228 in the watermarking system and procedure illustrated in Fig. 2A or Fig. 2B).

The limitation of claims 47-50 has been addressed above (see also figures 9 and 10)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to NANCY BITAR whose telephone number is (571)270-1041. The examiner can normally be reached on Mon-Fri (7:30a.m. to 5:00pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jinge Wu can be reached on 571-272-7429. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Jingge Wu/
Supervisory Patent Examiner, Art Unit 2624

Nancy Bitar 12/10/2008